EXHIBIT J

The New York Times https://www.nytimes.com/2018/02/18/technology/virtual-currency-extortion.html

Bitcoin Thieves Threaten Real Violence for Virtual Currencies

By Nathaniel Popper

Feb. 18, 2018

SAN FRANCISCO — The currency they were after was virtual, but the guns they carried were anything but.

In the beach resort of Phuket, Thailand, last month, the assailants pushed their victim, a young Russian man, into his apartment and kept him there, blindfolded, until he logged onto his computer and transferred about $100,000 worth of Bitcoin to an online wallet they controlled.

A few weeks before that, the head of a Bitcoin exchange in Ukraine was taken hostage and only released after the company paid a ransom of $1 million in Bitcoin.

In New York City, a man was held captive by a friend until he transferred over $1.8 million worth of Ether, a virtual currency second in value only to Bitcoin.

The rich have always feared robbery and extortion. Now, big holders of Bitcoin and its brethren have become alluring marks for criminals, especially since the prices of virtual currencies entered the stratosphere last year.

Virtual currencies can be easily transferred to an anonymous address set up by a criminal. While banks can stop or reverse large electronic transactions made under duress, there is no Bitcoin bank to halt or take back a transfer, making the chances of a successful armed holdup frighteningly enticing.

Thieves have taken advantage of this system in a startling number of recent cases, from Russia, Ukraine and Turkey to Canada, the United States and Britain.

“This is now becoming more pervasive and touching more law enforcement divisions that deal with organized crime and violent crime on a local level,” said Jonathan Levin, the founder of Chainalysis, which has worked with several law enforcement agencies on virtual currency crimes.

Mr. Levin’s company specializes in tracking criminal transactions on the blockchain, the computerized ledger where every Bitcoin transaction is publicly recorded.

Chainalysis has helped police attempt to track down criminals in several recent cases, including some that have not been made public, according to Mr. Levin.

But even when a transaction can be tracked, the design of Bitcoin means that criminals do not have to associate their identity with their Bitcoin address — as is necessary with most traditional bank accounts. That has stymied police in several cases.

Police in Phuket, Thailand, said attackers held a young Russian man in his apartment until he transferred about $100,000 worth of Bitcoin to their control. “We asked the victim how to track it since they know Bitcoin better than us,” one investigator said. “We asked them how to check the receiver. They said there is no way.” Chalong Police station

“For this, the advantage of Bitcoin is that it’s hard to verify,” said Chanut Hongsitthichaikul, an investigator with the Chalong Police Station, which investigated the case in Phuket. “We asked the victim how to track it since they know Bitcoin better than us. We asked them how to check the receiver. They said there is no way. It is hard to do.”

The Thai police tracked the victim’s laptop, which was also stolen, to Kuala Lumpur. That’s where the trail went cold.

While the recent crime wave has brought a new level of violence, virtual currency holders have been targets for several years. Criminals have been staging a long-running campaign to remotely hijack the cellphone numbers of prominent virtual currency holders in order to gain control of their digital wallets.

A few years ago, some of Bitcoin’s earliest proponents had SWAT teams called to their homes by people who demanded big Bitcoin payments to stop the harassment — a tactic called “SWATing” in some online communities.

There have also been many documented holdups around the world at in-person meetings where people were looking to convert cash into virtual currency, including one last year in Palm Beach, Fla., where the thief made off with $28,000 before being arrested.

But criminals have grown much more brazen as the price of Bitcoin has spiked.

The most audacious attack hit Exmo, the virtual currency exchange in Ukraine. The chief executive of the exchange, Pavel Lerner, was abducted the day after Christmas and freed a few days later after the company made a ransom payment of Bitcoin worth around $1 million.

A spokeswoman for Exmo said the money came from Mr. Lerner’s personal funds. Mr. Lerner was on leave from the company but would return.

A month earlier, a Turkish businessman was forced to hand over the passwords to his virtual currency wallets — containing nearly $3 million worth of Bitcoin — after having his car stopped by an armed gang in Istanbul that appeared to know about his Bitcoin holdings, according to local news reports.

Many big virtual currency holders privately say that they will no longer travel to Russia, Turkey or other countries where they assume that attacks may be easier to pull off because of organized crime.

But armed attackers have also hit a Canadian Bitcoin exchange in Ottawa, the Ether investor in New York City and a prominent virtual currency trader living near Oxford, England.

In a number of cases, the assailants have been caught — and forced to return money — because of video footage. In other cases, the criminals are still at large.

The unsolved crimes have sown fear among the ranks of the so-called crypto rich, which have grown considerably over the past year.

Bitcoin is the world’s most popular virtual currency. Such currencies are not tied to a bank or government and allow users to transfer money anonymously. Kin Cheung/Associated Press

At a conference for about 170 leaders in the virtual currency industry this month, there was a panel discussion about how to deal with the threat of robbery, extortion and kidnappings in which the criminals seek Bitcoin or other virtual currencies.

Organizers of the conference, known as the Satoshi Roundtable and held near Cancun, Mexico, brought in a security force and instituted significant privacy measures for guests to protect them from criminals while they were in attendance.

During the group discussion at the conference, attendees talked about having a “duress wallet” at home that can be handed over to throw an assailant off the trail of a bigger fortune, as well as several other security measures that can be used to deal with the threat.

Most of the crypto rich are loath to speak publicly about the risk of physical attacks, for fear of making themselves targets.

But Jameson Lopp, a longtime Bitcoin engineer and virtual currency holder, said the community should be proactive in confronting the threat, to let criminals know that people are taking steps to protect themselves.

Last summer, someone called a SWAT team to Mr. Lopp’s house to harass him. Since then, Mr. Lopp has installed closed-circuit cameras around his property and posted photos on Twitter of the automatic weapon he has at home.

In a more technical defensive measure, Mr. Lopp has long kept his virtual currency in so-called multisignature wallets created by the company he works for, BitGo. These wallets require multiple people to sign off on a transaction before the money can move.

Mr. Lopp will go even further later this year when he, his girlfriend and his dog move to a new home. He plans to “go dark” — not providing the address to anyone and using a post office box for deliveries. But he said even that will not fully banish his concerns.

“If you are rich and you own real estate, or stocks or a sports team, somebody can’t mug you and take your sports team away,” he said. “Having liquid crypto assets makes you much more attractive for that type of criminal attack.”

Mr. Levin said programmers are working to develop methods of signing virtual currency transactions that can quietly alert the authorities that a transaction is being made under duress — something like the hidden button under the bank teller’s desk.

But he said the most obvious way to thwart attackers is with wallets that require multiple signatures, and with less public discussion about owning virtual currencies.

Mr. Lopp said it is important to publicize the many ways in which virtual currency holders can fend off assailants so that criminals reconsider the likelihood of a successful attack.

“We’re in the very early days of this becoming a problem,” Mr. Lopp said. “The attackers are still trying to figure out what the risk-reward really is.”